

Echo expands its vulnerability-free container images to also include first-party Helm charts

Echo's vulnerability-free container images and new Helm charts provide a seamless, secure foundation for modern cloud environments.

NEW YORK, NY, UNITED STATES, January 19, 2026

/EINPresswire.com/ -- [Echo](#), the leader in AI-powered secure software infrastructure, today announced the release of its own first-party Helm charts, enabling organizations to adopt Echo's vulnerability-free container images with full compatibility and minimal operational change.



With the introduction of native Helm charts, Echo now delivers a complete, drop-in solution for teams running containers at scale. Organizations can maintain existing deployment patterns while strengthening security and accelerating compliance, without refactoring applications or introducing new tooling or workflow overhead.

“

As container ecosystems become more complex, security has to be built in, not bolted on. Our Helm charts extend that philosophy by making secure infrastructure easy to adopt.”

*Eilon Elhadad, Co-Founder
and CEO of Echo*

Recent shifts across the container ecosystem have impacted hundreds of millions of image pulls, forcing teams to reassess the stability, cost, and security of their base images. Many organizations estimate annual replacement costs for popular tools that have gone commercial to be between \$100,000 and \$500,000. Echo's fully compatible images and Helm charts offer a cost-effective and low-friction alternative, allowing teams to swap in secure-by-design images while preserving

operational continuity. Additionally, Echo's aggressive SLA delivers rapid remediation, with new vulnerabilities triaged within 24 hours and fixed within 7 days.

“We started Echo to give organizations a foundation they can trust,” said Eilon Elhadad, Co-Founder and CEO of Echo. “As container ecosystems become more complex, security has to be built in, not bolted on. Our Helm charts extend that philosophy by making secure infrastructure easy to adopt without changing how teams work.”

As the first AI-native OS, Echo's purpose-built agents work autonomously to create container base images from scratch and maintain them continuously. When a new vulnerability emerges anywhere in the world, Echo's purpose-built AI agents automatically research the issue, identify affected images, find or develop fixes from unstructured sources, apply patches, run comprehensive compatibility testing, and generate pull requests for human review. This automated approach allows a lean team to maintain hundreds of continuously secured images – a task that, using traditional methods, would require hundreds of engineers.

Echo images are also FIPS-validated and STIG-hardened, providing a secure, compliant foundation for organizations operating in regulated environments. By delivering images that are pre-aligned with stringent requirements, Echo helps teams accelerate compliance initiatives such as FedRAMP without adding any developer effort – reducing both time to authorization and long-term operational overhead.

To get started, teams can schedule a brief 1:1 call with a dedicated Echo product expert. Most organizations are able to roll out Echo images and Helm charts within days, immediately unlocking long-term improvements in security, compliance, and operational efficiency. Visit echo.ai to learn more about Echo's secure container images and Helm chart support.

Lazer Cohen
concrete.media
[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/884346060>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.